www.jusletter.ch

Sylvain Métille / David Raedler

Le RGPD et le sous-traitant suisse

Quelle application du Règlement général de protection des données à un sous-traitant établi hors de l'Espace économique européen ?

Loin d'être évidente, la question de l'application du RGPD aux traitements de données à caractère personnel confiés à un sous-traitant a mené à de nouvelles discussions suite à la publication, en fin d'année 2019, de la version finale de lignes directrices censées la clarifier – mais qui ont en réalité apporté de nouvelles zones d'ombre. Dans leur article, les auteurs rappellent les différents rôles intervenant dans un traitement de données à caractère personnel ainsi que les dispositions relatives au champ d'application territorial du RGPD, ceci avant d'examiner spécifiquement le cas du sous-traitant.

Catégories d'articles : Contributions
Domaines juridiques : Protection des données, Droit européen

Proposition de citation : Sylvain Métille / David Raedler, Le RGPD et le sous-traitant suisse, in : Jusletter 26 octobre 2020

Table des matières

1. Introduction

[1] Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après : **RGPD**) s'applique depuis le 25 mai 2018. Plus de deux ans après, certaines questions demeurent très discutées, dont celle de son champ d'application territoriale.

[2] À ce sujet, le Comité européen de la protection des données (ci-après : **EDPB**)[1] a publié en novembre 2019 la version finale de ses Lignes directrices 3/2018 sur le champ d'application territorial du RGPD (article 3)[2] (ci-après : **LD 3/2018**), censées aider à comprendre et interpréter l'art. 3 RGPD. Apportant des confirmations sur de nombreux points, les LD 3/2018 ne clarifient toutefois pas toutes les questions ouvertes, voire apportent de nouvelles zones d'ombre. Parmi celles-ci, la principale concerne la position défendue par les LD 3/2018 sur l'application extraterritoriale du RGPD aux sous-traitants spécifiquement. Modifiée en partie suite à la phase de consultation publique, cette position ne fait pas l'unanimité et laisse dubitatif à plusieurs égards. Pourtant, il s'agit là d'une question souvent centrale tant pour les sous-traitants que les responsables du traitement, notamment pour savoir quelles règles régissent leurs rapports ainsi que leurs obligations vis-à-vis des données à caractère personnel qui sont traitées. Cette importance nous amène à consacrer la présente contribution à ce thème, en se concentrant sur son aspect européen sous un spectre extraterritorial.

[3] Après un bref rappel des notions relatives aux différents acteurs impliqués dans un traitement de données à caractère personnel **(2)**, dont celle de sous-traitant, nous nous pencherons sur l'identification territoriale des règles applicables aux sous-traitants dans le RGPD **(3)**, avant de terminer avec quelques remarques conclusives **(4).** Il est précisé que la notion de « données à caractère personnelles » sera utilisée dans la présente contribution en raison de l'accent qui y

1 L'EDPB est un organe européen indépendant composé de représentants des autorités nationales chargées de la protection des données et du Contrôleur européen de la protection des données. Il contribue à l'application cohérente des règles en matière de protection des données au sein de l'UE (art. 68 ss RGPD).

2 *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, 12 novembre 2019*. Les références citées à la LD 3/2018 dans la présente contribution se réfèrent à la version originale en langue anglaise.

est mis sur le RGPD, où cette terminologie est utilisée (art. 4 ch. 1 RGPD). La notion est toutefois similaire à celle de « données personnelles » au sens du droit suisse.

2. Les acteurs du traitement de données à caractère personnel

[4] De façon très générale, un traitement de données à caractère personnel impliquera au moins deux acteurs : la personne concernée, qui bénéficie de différents droits[3], et le responsable du traitement, soumis à un lot d'obligations et de règles à respecter. Pourra s'y ajouter, selon les cas, un troisième acteur en la personne du sous-traitant (qui intervient pour le compte du responsable du traitement).

[5] Ces différents rôles peuvent encore connaître certaines particularités selon le type de traitement de données à caractère personnel qui est mis en œuvre. Ainsi, l'on peut notamment trouver en pratique le cas de responsables conjoints du traitement[4] ou de sous-traitants ultérieurs[5], pour ne prendre que deux exemples.

[6] Premier acteur dont la mention s'impose, la personne concernée est la personne[6] identifiée ou identifiable dont les données à caractère personnel sont traitées. Cette définition est commune au droit suisse (art. 3 let. b LPD) et au droit européen (art. 4 ch. 1 RGPD), à la différence essentielle que le droit suisse intègre également dans ce cadre les personnes morales – au contraire du droit européen et du pLPD qui se limitent aux personnes physiques[7].

[7] Une personne sera identifiée dès le moment où elle peut être directement reconnue sur la base des informations à disposition[8]. Tel sera essentiellement le cas lorsque ces informations comprennent une caractéristique propre telle que le nom, la signature ou l'image. Le caractère « identifié » d'une personne pourra également découler du contexte ou du contenu général des informations en question, lorsque leur lecture permet indéniablement une identification, sans que d'autres informations additionnelles n'aient à s'y ajouter[9].

---

3 Ces droits ne sont pas absolus et pourront trouver leurs limites en application des intérêts prépondérants d'autres personnes concernées par le traitement, qu'il s'agisse du responsable du traitement lui-même ou d'autres personnes.

4 On parle de responsables conjoints lorsqu'ils déterminent conjointement les finalités et les moyens du traitement conformément à l'art. 4 ch. 7 RGPD et l'art. 26 du projet du Conseil fédéral sur la révision totale de la loi fédérale sur la protection des données (ci-après : **pLPD**). Voir Mario Martini, in : Boris Paal/Daniel Pauly (édit.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2e éd., Munich 2018, art. 3 N 19 ; Livio di Tria, L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, in : sic ! 3/2020, pp. 127–128.

5 Parfois aussi appelé sous-traitant de deuxième rang.

6 Le droit suisse actuel protège les personnes physiques et morales (art. 3 let. b LPD). Avec l'entrée en vigueur de la LPD révisée, le droit suisse sera aligné sur le droit européen et seules les données à caractère personnel de personnes physiques seront protégées (art. 4 let. b pLPD et art. 4 ch. 1 RGPD). Les personnes morales pourront continuer à invoquer les règles en matière de protection des secrets de fabrication et commerciaux (art. 162 CP) ou les droits de la personnalité (art. 28 ss CC, dans la mesure évidement où la protection de la personnalité ne touche pas à des caractéristiques qui, en raison de leur nature, appartiennent seulement aux personnes physiques, cf. ATF 138 III 337, c. 6.1.).

7 Sous l'angle du RGPD : Peter Gola, in : Gola (édit.), DS-GVO Kommentar, 2e, Munich 2018, art. 4 N 23.

8 Philippe Meier, Protection des données : Fondements, principes généraux et droit privé, Berne 2011, N 431 ; Rolf Schwartmann/Robin L. Mühlenbeck, in : Schwartmann/Jaspers/Thüsing/Kugelmann (édit.), DS-GVO/BDSG, Heidelberg 2018, art. 4 N 20.

9 Manuel Klar/Jürgen Kühling, in : Jürgen Kühling/Benedikt Buchner (édit.), Datenschutz-Grundverordnung/BDSG Kommentar, 2e., Munich 2018, art. 4 N 18.

[8] Le critère du caractère « identifiable » étend pour sa part largement le cercle des informations qui peuvent entrer dans la notion de données à caractère personnel – et dès lors des personnes qui peuvent être qualifiées de « personnes concernées ». Ainsi, une personne sera identifiable dès le moment où les informations à disposition ne suffisent elles-mêmes pas à l'identifier (contrairement à ce qui vaut dans le premier cas), mais que leur croisement avec d'autres informations y mènerait[10]. À titre d'exemple récent, l'on peut mentionner le cas d'une entreprise de taille moyenne au sein de laquelle tout employé se voit prendre sa température à l'entrée dans le cadre de mesures visant à lutter contre le coronavirus. Lorsque ces prises de température sont notées avec l'heure de l'examen, la personne pourra être « identifiable » même lorsque son nom n'est pas inscrit, par exemple en croisant cette information avec la journalisation des connexions au réseau informatique ou avec les images de vidéosurveillance. La seule connaissance de la personne par celle prenant la température pourrait également réaliser ce critère.

[9] En pratique, il est admis que les possibilités de croisement – et donc d'identification de la personne concernée – doivent être appréciées de façon très large. Ainsi, ce ne serait qu'en cas d'absolue impossibilité d'identifier une personne physique que l'absence du caractère identifiable, et donc d'une personne concernée, sera admise[11]. Dans ce contexte, et afin d'éviter d'étendre sans limite le champ d'application des règles en matière de protection des données à caractère personnel, l'on retient la possibilité *raisonnable* ou *vraisemblable* d'identifier la personne concernée, en ligne avec la précision expressément donnée au considérant 26 RGPD[12]. Seront dans ce cadre pris en compte les facteurs objectifs qui permettraient une telle identification, dont les coûts y relatifs, le temps nécessaire ainsi que la technologie existant au moment de l'appréciation[13]. Bien que la question soit encore discutée et controversée, la possibilité concrète d'accéder aux informations complémentaires nécessaires pour identifier la personne concernée devrait également être pertinente[14]. Avec certaines limites, le caractère identifiable d'une personne concernée pourra néanmoins être admis également si ces informations complémentaires ne sont accessibles qu'indirectement – soit par le biais d'un tiers, par exemple un fournisseur de services de télécommunication pour une adresse IP[15] – ou après la levée d'un obstacle existant[16].

[10] Le deuxième acteur est le responsable du traitement. La LPD actuelle parle de « maître du fichier » (art. 3 let. i LPD), alors que le RGPD utilise le terme de responsable du traitement (art. 4 ch. 7 RGPD) comme certains droit cantonaux et la LPD révisée (art. 4 let. i pLPD). Les deux termes sont utilisés ici de manière équivalente. Le responsable du traitement est défini comme étant en substance la personne[17] qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (données à caractère personnelles concernées, moyens utilisés et buts poursuivis).

---

10 Stefan Ernst, in : Paal/Pauly (édit.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2e éd., Munich 2018, art. 4 N 3 ; Klar/Kühling (note 9), art. 4 N 19 ; Meier (note 8), N 432.

11 Ernst (note 10), art. 4 N 9.

12 Ernst (note 10), art. 4 ; Klar/Kühling (note 9), art. 4 N 20 ; Schwartmann/Mühlenbeck (note 8), art. 4 N 28 et 29.

13 Ernst (note 10), art. 4 N 10 ; Klar/Kühling (note 9), art. 4 N 21 et 24.

14 Voir notamment l'arrêt CJUE C-582/14 du 19 octobre 2016 (Breyer), ainsi qu'en droit suisse l'arrêt du Tribunal fédéral 4A_365/2017 du 26 février 2018, c. 5. Notant toutefois le débat à ce sujet : Klar/Kühling (note 9), art. 4 N 25 ; Schwartmann/Mühlenbeck (note 8), art. 4 N 27 et 28.

15 Pour cette mention : Klar/Kühling (note 9), art. 4 N 35.

16 Ernst (note 10), art. 4 N 11.

17 Une personne physique, une personne morale ou une autorité publique.

[11] Le troisième acteur enfin est le sous-traitant[18]. C'est un acteur *possible* mais non nécessaire du traitement de données à caractère personnel. Le sous-traitant ne traite pas les données pour son propre compte, mais pour le compte du responsable du traitement et sur ses instructions[19]. Ce n'est donc pas lui – mais le responsable du traitement – qui décide des caractéristiques et modalités du traitement de données à caractère personnel, dont les catégories collectées et traitées ainsi que les buts poursuivis dans ce cadre. Il n'a donc aucune marge de manœuvre ou liberté dans le traitement entrepris par le responsable du traitement, intervenant comme une sorte de « marionnette »[20] ou le « prolongement » du responsable du traitement[21].

[12] Simple sur le principe, cette définition et l'identification exacte des sous-traitants peuvent parfois s'avérer difficiles à interpréter en pratique. Ceci en particulier dans la mesure où un fournisseur ou « sous-traitant » au sens contractuel du terme – par exemple un mandataire intervenant pour le compte du responsable du traitement – pourra ne pas être un « sous-traitant » au sens du droit de la protection des données. Ainsi, si le tiers intervenant dispose d'une grande marge de manœuvre pour décider du traitement de données à faire, notamment car il est compétent pour identifier les catégories de données à caractère personnel traitées, il sera par principe qualifié non pas de sous-traitant, mais bien de responsable du traitement. Tel sera également le cas si le tiers n'est pas spécifiquement mandaté pour traiter des données à caractère personnel, mais que ce traitement n'intervient qu'à titre accessoire pour exécuter le mandat principal.

[13] À titre d'exemple, tel sera le cas d'un avocat intervenant au profit de son client, dans la mesure où c'est bien lui qui décide du type d'informations dont il a besoin pour mener à bien son mandat. C'est également lui qui, par la procuration reçue, peut décider de certains traitements de données à caractère personnel particuliers, là également nécessaires pour sa mission. Un autre exemple peut être le comptable ou le fiduciaire qui est chargé de tenir et vérifier la comptabilité ou les déclarations fiscales d'une entreprise. Devant là également identifier les informations requises pour son mandat, il sera le plus souvent vu et qualifié de responsable du traitement et non de sous-traitant[22].

[14] La sous-traitance implique certaines exigences formelles, dont l'existence d'un contrat[23]. Il est précisé dans ce cadre que, tant dans la LPD que dans le RGPD, la conclusion du contrat est une exigence déclarative à respecter et ne revêt pas un effet constitutif[24]. Cependant, il s'agit bien d'une obligation qui doit être respectée – au risque sinon pour les parties d'enfreindre leurs

18 Art. 4 let. j pLPD et art. 4 ch. 8 RGPD

19 Meier (note 8), N 1196.

20 Pour cette expression : Ernst (note 10), art. 4 N 56.

21 Martini (note 4), art. 28 N 2.

22 Pour ces exemples et d'autres situations, voir notamment le document élaboré par le Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, notamment p. 28 (exemple de l'avocat) et p. 29 (exemple du comptable) ; Jürgen Hartung, in : Kühling/Buchner (édit.), Datenschutz-Grundverordnung/BDSG Kommentar, 2e éd., Munich 2018, art. 28 N 27. Il est à noter que le EDPB est actuellement en train de réviser la ligne directrice précédemment adoptée par le Groupe de travail « Article 29 » sur la protection des données, en ayant soumis à la consultation publique son projet de Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

23 À moins qu'une loi ne prévoie la sous-traitance, ce qui est rare. Voir les art. 10a LPD, art. 8 pLPD et art. 28 RGPD.

24 Hartung (note 22), art. 28 N 61. La violation des obligations de l'art. 28 RGPD peut mener au prononcé d'une amende administrative conformément à l'art. 83 par. 4 let. a RGPD ; Hartung (note 22), art. 28 N 101. À l'inverse, le droit suisse ne prévoit pas une conséquence similaire.

devoirs légaux. À noter également que cette exigence s'applique aussi à tout rapport de sous-traitance ultérieure qui serait noué par le sous-traitant lui-même (*subprocessing*)[25].

[15] Le RGPD exige la forme écrite, y compris sous forme d'échanges électroniques[26], ainsi que la présence d'un certain nombre d'éléments dans le contrat[27]. Conformément à l'art. 28 par. 3 RGPD, il doit définir l'objet et la durée du traitement, sa nature et finalité, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et droits du responsable du traitement et du sous-traitant. Sur ce dernier point, il dresse un catalogue des obligations qui doivent impérativement être précisées dans le contrat. Afin d'assurer que toutes les dispositions nécessaires sont bien contractuellement prévues, l'art. 28 par. 7 et 8 RGPD prévoit la possibilité pour la Commission européenne, ou les autorités nationales de contrôle, d'établir des clauses contractuelles types en la matière[28]. Sous l'angle du droit suisse, et au contraire du RGPD, aucun contenu impératif n'est légalement imposé dans la LPD (art. 10a) ou dans le pLPD.

3. L'application du RGPD au sous-traitant

3.1. Historique et processus parlementaires

[16] Comme cela sera détaillé au paragraphe 3.2, l'art. 3 RGPD prévoit essentiellement trois hypothèses différentes quant à son application territoriale, séparées en ses trois paragraphes. Dans l'ensemble, l'art. 3 RGPD était déjà prévu dans le projet initial du RGPD et n'a subi que quelques modifications dans le processus de discussion et d'adoption du texte final[29]. Ces modifications s'avèrent pertinentes pour l'analyse qui suit, de sorte qu'il est nécessaire d'y consacrer un bref développement.

[17] Concernant l'art 3 par. 1 RGPD, une seule modification est intervenue dans ce cadre, sur proposition du Parlement européen[30]. Une précision a été apportée quant au fait que le lieu géographique du traitement n'était dans ce cadre pas pertinent, seul comptant l'existence d'un établissement dans l'EEE[31]. Cette précision a été apportée par l'ajout d'une phrase en fin de paragraphe, selon laquelle l'application du RGPD intervient « *que le traitement ait lieu ou non dans l'Union* »[32].

[18] L'art. 3 par. 2 RGPD a subi des modifications plus marquées que le par. 1 lors des débats. Parmi les changements importants, l'un en particulier a été apporté quant au cercle des personnes visées par cette disposition à l'art. 3 par. 2 let. a RGPD. Sur proposition du Parlement

25 Hartung (note 22), art. 28 N 89.

26 Une réserve qui figure d'ailleurs explicitement à l'art. 28 par. 9 RGPD ; Hartung (note 22), art. 28 N 95 ; Christoph Klug, in : Gola (édit.), DS-GVO Kommentar, 2e, Munich 2018, art. 28 N 12. Également Sascha Kremer, in : Schwartmann/Jaspers/Thüsing/Kugelmann (édit.), DS-GVO/BDSG, Heidelberg 2018, art. 28 N 87.

27 Pour le détail : Hartung (note 22), art. 28 N 64 ss.

28 À ne pas confondre avec les clauses contractuelles types liées au transfert international de données à caractère personnel en application des art. 46 par. 2 let. d RGPD.

29 Daniel Ennöckl, in : Gernot Sydow (édit.), Datenschutzgrundverordnung, Handkommentar, 2e éd., Baden-Baden 2018, art. 3 N 3.

30 Constatant le peu de modifications apportées : Manuel Klar, in : Kühling/Buchner (édit.), Datenschutz-Grundverordnung/BDSG Kommentar, 2e éd., Munich 2018, art. 3 N 30.

31 Si le texte du RGPD parle du territoire de l'Union, il faut comprendre qu'il s'agit de l'EEE en application de la Décision du Comité mixte de l'EEE 154/2018 du 6 juillet 2018.

32 Ennöckl (note 29), art. 3 N 3.

européen, une référence explicite au « sous-traitant » y a ainsi été intégrée en cours de discussion[33]. Un autre changement a pour sa part visé l'art. 3 par. 2 let. b RGPD, par lequel toute forme de « suivi du comportement » d'une personne dans l'EEE était visée et non uniquement une véritable surveillance[34]. Cette dernière éventualité, plus restrictive, avait été proposée dans le cadre des discussions par-devant le Parlement européen, sans pour autant être confirmée[35]. Enfin, le rattachement à l'EEE qui y était fait par référence à la « résidence » (*residing* ; *ansässig*) a été remplacée par la seule mention au fait de « se trouver » dans l'EEE[36].

[19] Alors que ces changements revêtent une grande importance, à l'image de l'art. 3 par. 2 RGPD dans son ensemble, le matériel lié aux débats parlementaires ainsi qu'à l'adoption du RGPD n'offre quasiment aucune clé d'interprétation à son sujet[37]. Ceci alors que cette disposition fait appel à plusieurs concepts juridiques indéterminés et nouveaux – lesquels ne sont pas plus explicités ou détaillés dans le matériel précité.

[20] S'agissant spécifiquement des LD 3/2018, une première version a été mise en consultation publique le 16 novembre 2018 et elles ont été adoptées de façon définitive le 12 novembre 2019. Plusieurs changements et précisions ont été apportés au texte des LD 3/2018, tant sur les exemples donnés que sur certains développements au fond. En ce qui concerne le sous-traitant, on peut mentionner les points suivants :

- l'art. 3 RGPD vise à clarifier si une activité de traitement est soumise au RGPD, et non spécialement si une personne entre dans son champ d'application territoriale – menant en conséquence à retenir qu'une même personne pourra être soumise au RGPD pour certaines de ses activités de traitement et non pour d'autres[38] ;
- la présence d'un employé dans l'EEE n'amène pas impérativement à retenir l'existence d'un établissement au sens de l'art. 3 par. 1 RGPD[39] ;
- le caractère « volontaire » du ciblage est requis par l'art. 3 par. 2 RGPD[40] ;
- quelques précisions quant à la nomination du représentant dans l'EEE et à sa responsabilité personnelle[41] ;
- l'apparition de développements relatifs aux conséquences pour le sous-traitant d'une soumission du responsable du traitement au RGPD par le truchement de l'art. 3 par. 2 RGPD[42].

33 Ennöckl (note 29), art. 3 N 3 et 31.

34 Relevant le changement lié au fait que le Parlement européen souhaitait que la surveillance en question ne soit pas uniquement celle sur Internet, Klar (note 30), art. 3 N 33.

35 Ennöckl (note 29), art. 3 N 3.

36 Klar (note 30), art. 3 N 31 et 64.

37 Klar (note 30), art. 3 N 3.

38 LD 3/2018, pp. 5 et 14.

39 LD 3/2018, p. 6.

40 LD 3/2018, pp. 15 et 18.

41 LD 3/2018, pp. 24 à 28.

42 LD 3/2018, pp. 20 à 22.

3.2. Les différentes hypothèses visées par l'art. 3 RGPD

[21] Alors que le champ d'application matériel du RGPD est précisé à l'art. 2 et ne fait l'objet que de peu de débats[43], le champ d'application territorial du RGPD est pour sa part donné à l'art. 3 RGPD. Dans la ligne de la précision explicitement apportée par l'EDPB aux LD 3/2018 suite à la consultation publique, ces hypothèses se concentrent sur les *types de traitement* plutôt que sur la personne l'effectuant[44]. En d'autres termes, un même sous-traitant pourra être soumis au RGPD pour certains de ses traitements – essentiellement sous l'angle de l'art. 3 par. 2 RGPD – et non pour d'autres[45], étant néanmoins précisé que certaines des obligations prévues dans le RGPD s'appliqueront intégralement dès qu'il y a soumission au RGPD. Tel sera le cas notamment de l'obligation de nommer un représentant dans l'UE (art. 27 RGPD) ou de celle de nommer un délégué à la protection des données à caractère personnel (art. 37 et 38 RGPD).

3.2.1. Application territoriale du RGPD (art. 3 par. 1 RGPD)

[22] La première – et principale[46] – application est celle couverte par l'art. 3 par. 1 RGPD, soit l'application fondée sur l'existence d'un établissement dans l'EEE. Ce « critère de l'établissement »[47] dispose que le RGPD est applicable à tout traitement de données effectué par un responsable du traitement ou un sous-traitant dans le cadre des activités d'un établissement dans l'EEE[48]. Il y est explicitement précisé que le lieu exact du traitement[49] ou le lieu de résidence ou de situation de la personne concernée[50] ne sont pas pertinents. Le RGPD s'appliquera ainsi également à un traitement intervenant hors de l'EEE, mais dans le cadre des activités de l'établissement dans l'EEE.

[23] Dans le cas où le sous-traitant est établi dans l'EEE, ses activités de traitement y seront soumises de la même manière, que le responsable du traitement se trouve sur le territoire de l'EEE ou en dehors[51].

3.2.2. Application extraterritoriale du RGPD (art. 3 par. 2 RGPD)

[24] La seconde application vise un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'EEE (art. 3 par. 2 RGPD). Fondée sur le critère du *lieu du marché* (*Marktortprinzip*)[52]

---

43 Pour une analyse : Sylvain Métille/Annelise Ackermann, RGPD : application territoriale et extraterritoriale, in : Epiney/Rovelli (édit), Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen = Le règlement général sur la protection des données (RGPD) : portée et premières expériences, Zurich/Bâle/Genève 2020, p. 78.

44 LD 3/2018, pp. 5 et 14.

45 Explicitement LD 3/2018, p. 14.

46 Ennöckl (note 29), art. 3 N 1.

47 Voir sur ce point la terminologie utilisée dans LD 3/2018, p. 4 (*establishment criterion*).

48 Métille/Ackermann (note 43), pp. 79–81 ; Philipp Mittelberger, Der Extraterritoriale Ansatz der Datenschutzgrundverordnung (DS-GVO), 2018, p. 9 ; Dan Jerker Svantesson, in : Kuner/Bygrave/Docksey (édit.), The General Data Protection Regulation (GDPR) – A commentary, Oxford 2019, pp. 81 et 86.

49 Ce même principe découle également du considérant 22.

50 Klar (note 30), art. 3 N 36, relevant que la nationalité n'est elle-même pas non plus pertinente ; également Métille/Ackermann (note 43), p. 81.

51 Le lieu où se trouve le sous-traitant n'a en revanche pas d'influence sur l'application du RGPD au responsable du traitement.

52 Klar (note 30), art. 3 N 6 ss.

ou du « ciblage »[53], elle ne s'applique toutefois que si deux conditions cumulatives sont réalisées[54].

[25] Premièrement, les données à caractère personnel traitées doivent être « relatives à des personnes concernées qui se trouvent sur le territoire de l'EEE ». Le RGPD assure ainsi un rattachement géographique à l'EEE. Il ne précise en revanche pas ce qu'il convient d'entendre par « se trouver » sur le territoire de l'EEE, notamment si cela implique ou non un critère stable et inscrit dans le temps[55]. Compte tenu à la fois des changements apportés au cours du processus d'adoption du RGPD[56] et de la référence explicite au fait de « se trouver » dans l'EEE, sans complément impliquant une quelconque durée ou le caractère stable de la situation, il est admis que la seule présence dans l'EEE suffit pour réaliser cette première condition[57], et cela indépendamment de la nationalité ou du lieu de domicile – ou de résidence – de la personne concernée.

[26] Deuxièmement, il est nécessaire que l'une des deux situations listées aux let. a et b de l'art. 3 par. 2 RGPD soit réalisée et que les activités de traitement soient liées :

- à l'offre de biens ou de services à des personnes concernées dans l'EEE, qu'un paiement soit exigé ou non ; ou
- au suivi du comportement de personnes concernées lorsque ce comportement se déroule au sein de l'EEE.

[27] S'agissant tout d'abord de la première situation, elle vise à éviter un *forum shopping*, soit le fait pour une entreprise de se baser volontairement en dehors de l'EEE afin d'éviter une application du RGPD, tout en visant spécifiquement les consommateurs européens[58]. Elle couvre ainsi toutes les formes de distribution de biens et services, y compris par le commerce en ligne[59]. Le RGPD ne s'applique donc pas à toute activité de traitement d'une entité non européenne, ni même à toute entité dont les biens ou les services pourraient être utilisés ou consommés par une personne résidant dans l'EEE. Il est au contraire nécessaire que l'offre en question *vise* des personnes qui se trouvent dans l'EEE[60]. Comme cela a explicitement été ajouté par l'EDPB à la suite de la consultation publique des LD 3/2018, ce critère implique donc la *volonté* de viser ces personnes, le seul fait qu'elles puissent se trouver dans l'EEE n'amenant pas à une application du RGPD[61].

[28] D'un point de vue international, le critère du lieu du marché a déjà fait couler beaucoup d'encre et a accru les craintes des entreprises de se voir très largement soumises à ce Règle-

53 LD 3/2018, p. 4, étant précisé que nous ne rejoignons pas cette terminologie pour couvrir les deux cas couverts par l'art. 3 par. 2 RGPD, compte tenu du fait – comme cela sera précisé *infra* – que le cas du suivi du comportement de l'art. 3 par. 2 let. b RGPD ne nécessite justement pas de ciblage particulier.

54 Métille/Ackermann (note 43), p. 82.

55 Klar (note 30), art. 3 N 63 ; Métille/Ackermann (note 43), p. 83.

56 Cf. *supra* 3.1.

57 Klar (note 30), art. 3 N 64 ; Heinz-Joachim Pabst, in : Schwartmann/Jaspers/Thüsing/Kugelmann (édit.), DS-GVO/BDSG, Heidelberg 2018, art. 3 N 22 ; Svantesson (note 48), p. 88.

58 Klar (note 30), art. 3 N 18 ; Pabst (note 57), art. 3 N 26.

59 Klar (note 30), art. 3 N 6 et 10.

60 Ennöckl (note 29), art. 3 N 13 et 14 ; Klar (note 30), art. 3 N 9 et 19.

61 LD 3/2018, p. 15. Critiquant une expansion trop importante liée à l'art. 3 par. 2 let. a RGPD : Paul de Hert/Michal Czerniawski, Expanding the European data protection scope beyond territory : Article 3 of the General Data Protection Regulation in its wider context, International Data Privacy Law, 2016, Vol. 6, No. 3, p. 240 et 241.

ment, bien qu'il ne s'agisse pas d'une nouveauté dans l'ordre juridique. D'abord, car il existe dans d'autres domaines que le droit de la protection des données, notamment en droit de la concurrence ou en droit des marchés financiers[62]. Ensuite, car plusieurs autres États appliquent ce critère également en droit de la protection des données. Tel est par exemple le cas aux États-Unis d'Amérique où *la Federal Trade Commission* (FTC) a plusieurs fois utilisé le critère du « ciblage » (*Targeting criteria*) afin d'imposer ses compétences ainsi que l'application du droit américain[63].

[29] La deuxième situation vise le « suivi du comportement », et n'exige pas un ciblage particulier des personnes dans l'EEE[64]. L'unique critère d'application est celui du suivi d'un comportement dans l'EEE, y compris donc lorsque ce suivi n'est pas voulu ou même souhaité par le responsable du traitement ou le sous-traitant. Cet élément est d'ailleurs critiqué en littérature, dans la mesure où il peut dans les faits entraîner une application du RGPD à l'échelle mondiale[65]. Tel serait notamment le cas pour tout site web disposant de *cookies* qui opéreraient un suivi du comportement des visiteurs[66]. Dans la mesure où aucun ciblage spécifique n'est requis, le simple fait de disposer d'un tel site web pourrait d'ores et déjà suffire pour entrer dans le champ d'application du RGPD par le biais de son art. 3 par. 2 let. b. Bien que ce risque existe, vu la formulation très ouverte de l'art. 3 par. 2 RGPD sur ce point, la grande majorité de la doctrine est d'avis de prendre en compte là également le but du responsable du traitement ou du sous-traitant. Cette position semble également partagée dans les LD 3/2018[67].

[30] Le fait que le RGPD requiert bien la réalisation de deux conditions cumulatives – et non uniquement du critère de la présence de la personne concernée dans l'EEE – évite qu'il ne s'applique à tout traitement concernant une personne résidant dans l'EEE. Les critères de « l'offre d'un bien ou d'un service » et du « suivi du comportement » permettent de limiter l'étendue du champ d'application du RGPD[68]. En d'autres termes, seuls des traitements qui présentent un lien réel et suffisant avec l'EEE se voient couverts par le RGPD[69]. Nous verrons cependant au paragraphe 3.3 que le champ d'application du RGPD au sous-traitant pose encore d'importants problèmes, y compris par rapport à ce rattachement.

3.2.3. Application par renvoi au droit européen (art. 3 par. 3 RGPD)

[31] Avant d'examiner la situation spécifique du sous-traitant, il est encore utile de mentionner qu'une troisième application est aussi visée par l'art. 3 RGPD, cette fois à son troisième paragraphe. Il y est prévu que le RGPD s'applique à tout traitement de données par un responsable du traitement qui n'est pas établi dans l'EEE, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public. Cette application concerne principalement les

62 Sous l'angle du droit européen, Klar (note 30), art. 3 N 6.

63 Klar (note 30), art. 3 N 7.

64 Klar (note 30), art. 3 N 23 ; Métille/Ackermann (note 43), p. 87.

65 Klar (note 30), art. 3 N 24.

66 C'est le cas des cookies dit « marketing ».

67 LD 3/2018, p. 20.

68 Pour ce même constat Klar (note 30), art. 3 N 19, qui relève bien l'utilité de cette double-condition.

69 Klar (note 30), art. 3 N 21.

cas dans lesquels le traitement est effectué par une représentation diplomatique ou consulaire qui est soumise, en vertu du droit international, au droit d'un État membre[70].

[32] Au contraire de ce qui vaut pour les deux premiers paragraphes de l'art. 3, l'art. 3 par. 3 RGPD ne porte expressément que sur les traitements de données par un « responsable du traitement », sans se référer aux sous-traitants. Pourtant, il n'est pas exclu que l'hypothèse couverte par cette troisième application puisse également concerner un sous-traitant. Tel serait par exemple le cas si une représentation diplomatique intervient comme sous-traitant pour une autre entité représentant le pays, voire pour un autre État.

3.3. Conséquences pour le sous-traitant en particulier

[33] Le champ d'application territorial du RGPD ainsi rappelé, il est nécessaire d'en donner une lecture spécifique au sous-traitant, afin de couvrir les différentes hypothèses qui peuvent se poser en pratique. Chacune d'elles sera ici évoquée et distinguée, afin de clarifier à chaque fois les conséquences sous l'angle de l'application du RGPD.

3.3.1. Sous-traitant disposant d'un établissement dans l'EEE

[34] La première hypothèse possible concerne le sous-traitant établi dans l'EEE, c'est-à-dire disposant d'un établissement au sens de l'art. 3 par. 1 RGPD. Dans un tel cas, il devra respecter les obligations revenant au sous-traitant selon le RGPD pour toutes ses activités de traitement entrant dans le cadre des activités de l'établissement dans l'EEE[71]. Ceci à l'image de toute personne dont les activités de traitement sont matériellement soumises au RGPD et qui, territorialement, les exerce dans le contexte des activités d'un établissement dans l'EEE.

[35] Ce principe et l'application générale du RGPD vaudront indépendamment de la question de savoir si le responsable du traitement ou la personne concernée sont eux-mêmes basés dans l'EEE[72]. Autrement dit, un sous-traitant disposant d'un établissement dans l'EEE qui serait mandaté par un responsable du traitement basé pour sa part hors de l'EEE (par exemple en Suisse) restera entièrement soumis au RGPD pour les activités effectuées dans ce cadre[73]. À l'inverse, cela n'entraînera pas l'application directe du RGPD au responsable du traitement basé en dehors de l'EEE ou, plus précisément, aux traitements que le responsable du traitement effectue dans ce cadre. En particulier, il est admis que le sous-traitant dans l'EEE ne saurait être vu comme agissant en tant qu'« établissement » du responsable du traitement situé hors de l'EEE[74]. Selon les cas, une application du RGPD basée sur son art. 3 par. 2 reste en revanche envisageable à son égard.

[36] Cela étant, il est important de relever que le seul fait que le sous-traitant soit soumis dans ce cadre au RGPD n'amènera pas nécessairement à une application directe du RGPD au traite-

70 Svantesson (note 48), pp. 92–93.

71 La référence aux traitement entrant dans « le contexte » des activités d'un établissement dans l'EEE est nécessaire dans le cadre de l'art. 3 par. 1 RGPD.

72 Klar (note 30), art. 3 N 2.

73 LD 3/2018, p. 10.

74 Klar (note 30), art. 3 N 38 ; explicitement également en pp. 10–12 des LD 3/2018.

ment qui lui est confié. En effet, seules les obligations revenant personnellement au sous-traitant seront applicables dans un tel cas, à l'exclusion naturellement des obligations prévues pour le responsable du traitement ou, possiblement, des droits de la personne concernée. Le détail des obligations alors applicables est donné dans les LD 3/2018 comme portant sur les obligations suivantes du sous-traitant :

- l'obligation de conclure un contrat écrit de sous-traitance (art. 28 RGPD) ;
- les obligations lui revenant explicitement selon l'art. 28 par. 2 à 6 RGPD, notamment par rapport à ses propres sous-traitants ;
- la soumission aux instructions du responsable du traitement, évidemment d'une façon conforme à ses propres obligations ;
- la tenue d'un registre des activités de traitement (art. 30 par. 2 RGPD) ;
- l'obligation de coopérer avec l'autorité (art. 31 RGPD) ;
- la mise en œuvre de mesures techniques et organisationnelles assurant la sécurité des données à caractère personnel (art. 32 RGPD) ;
- les obligations d'information en cas de faille de sécurité, qui ne couvre cependant qu'une information au responsable du traitement et non à la personne concernée directement ou à l'autorité (art. 33 RGPD) ;
- la nomination d'un délégué à la protection des données à caractère personnel (art. 37 et 38 RGPD) ; et
- les limites et contraintes en cas de transmission de données à caractère personnel à l'étranger (chapitre V du RGPD)[75].

[37] À l'inverse, plusieurs obligations ne s'appliqueront pas au sous-traitant pour le traitement en question. Tel sera par exemple le cas des obligations en matière d'analyse d'impact relative à la protection des données (art. 35 RGPD), des obligations de consultation préalable (art. 36 RGPD) ou encore des obligations liées à l'information de la personne concernée (art. 12 et 13 RGPD). Toutes ces obligations reviennent en effet au responsable du traitement et non au sous-traitant.

[38] Alors que l'on peut rejoindre les LD 3/2018 sur l'essentiel de ces développements, l'obligation imposée au sous-traitant de conclure un contrat écrit de sous-traitance peut amener à une contradiction par rapport aux développements des LD 3/2018 ainsi qu'au texte du RGPD. En effet, dans un tel cas, il reviendrait au sous-traitant d'imposer un contrat complet au responsable du traitement, reprenant les obligations de l'art. 28 RGPD. Or, cela mènerait justement à soumettre contractuellement le responsable du traitement aux obligations du RGPD y évoquées[76].

[39] Une particularité doit encore être évoquée spécialement sous l'angle des limites et contraintes en cas de transmission de données à caractère personnel à l'étranger. Ce cas pourra en effet s'avérer problématique vu justement les limites posées dans le RGPD, lorsque la communication de données à caractère personnel intervient du sous-traitant (dans l'EEE) au responsable du traitement (hors EEE). Malgré la prévalence pratique du cas et la mention, dans les LD 3/2018, du

75 LD 3/2018, pp. 12 et 13.

76 Relevant le problème : Christopher Millard/Dimitra Kamarinou, in : Christopher Kuner/Lee Bygrave/Christopher Docksey (édit.), The General Data Protection Regulation (GDPR) – A commentary, Oxford 2019, p. 609.

fait que le Chapitre V RGPD est applicable aux transferts effectués par le sous-traitant, aucune référence n'y est faite à ce cas spécifique. Or, la majorité de la doctrine retient que, sous l'angle du RGPD, une telle communication constitue bien un « transfert » à un tiers[77]. Et un tel transfert pourra être problématique dans tous les cas où le responsable du traitement ne se trouve pas dans un État qui ferait l'objet d'une décision d'adéquation selon l'art. 45 RGPD.

[40] Confronté à une telle situation, le sous-traitant devra soumettre tout transfert au responsable du traitement à l'obtention de garanties appropriées selon l'art. 46 RGPD ou se trouver dans l'une des situations particulières de l'art. 49 RGPD. À défaut, et alors même que le sous-traitant est mandaté par le responsable du traitement pour effectuer les traitements en question, il ne saurait enfreindre ses propres obligations en ne respectant pas ces limitations. À noter toutefois que ces limitations ne devraient pas s'appliquer lorsque les données à caractère personnel concernées ont déjà fait l'objet d'une transmission du responsable du traitement au sous-traitant ou qu'elles sont déduites d'une telle transmission, par exemple suite à leur analyse par le sous-traitant.

3.3.2. Sous-traitant ne disposant pas d'un établissement dans l'EEE

[41] La seconde hypothèse concerne le cas dans lequel le sous-traitant est établi hors de l'EEE. Afin de comprendre les conséquences de l'art. 3 par. 2 RGPD pour le sous-traitant, deux cas de figure doivent être séparés selon que l'application extraterritoriale découlerait des actions du sous-traitant lui-même (soumission par ses propres activités) ou se fonderait uniquement sur les activités de traitement entreprises pour le compte du responsable du traitement (soumission par les activités pour le compte du responsable du traitement).

[42] Dans le premier cas de figure, le sous-traitant se verrait personnellement appliquer le RGPD de façon extraterritoriale en raison de ses propres actions. Ceci car, de son côté, il déciderait de viser une des personnes concernées sur le territoire de l'EEE pour leur offrir ses biens ou services, ou choisirait de suivre le comportement de ces personnes.

[43] Cette hypothèse, naturellement possible vu le fait que le sous-traitant déploie ses propres activités, amène cependant à en faire un responsable du traitement – et non plus un sous-traitant. En effet, comme vu ci-avant, l'existence d'un sous-traitant suppose justement que celui-ci ne décide pas lui-même des activités de traitement à faire, mais est instruit pour cela par le responsable du traitement. S'il vient lui-même à décider de traitements – ou à faire ses propres traitements pour ses propres buts – il sera qualifié de responsable du traitement. À titre d'exemple, le sous-traitant qui promouvrait des services d'hébergement numérique (*hosting*), dans le but de rechercher des clients, sera pour ce traitement un responsable du traitement. Si les clients recherchés sont des individus se trouvant dans l'EEE, le critère de l'art. 3 par. 2 RGPD sera très vraisemblablement réalisé – mais en sa qualité de responsable du traitement. Cela ne présuppose toutefois pas la qualification à réserver aux activités de traitement qu'il déploierait par la suite, *pour le compte* de ses propres clients. Par exemple, pour reprendre le cas précité, par les données que le client sauvegarderait sur les serveurs du sous-traitant et qui seraient liées à d'autres personnes concernées.

[44] Dans le deuxième cas de figure, le sous-traitant est hors de l'EEE et le responsable du traitement est soumis au RGPD, de manière territoriale ou extraterritoriale.

77 Klar (note 30), art. 3 N 38.

(i) Le responsable du traitement soumis au RGPD en raison d'un établissement dans l'EEE (art. 3 par. 1 RGPD)

[45] Compte tenu du fait qu'un responsable du traitement soumis au RGPD sous l'angle de l'art. 3 par. 1 RGPD y demeure lié indépendamment du lieu dans lequel se fait le traitement de données, le fait pour celui-ci d'être confié à un sous-traitant hors de l'EEE n'aura pas pour conséquence de le sortir du champ d'application du RGPD[78]. Mais cela n'entraîne pas plus l'application directe du RGPD au sous-traitant.

[46] Le responsable du traitement devra en revanche soumettre contractuellement le sous-traitant à l'essentiel des obligations prévues dans le RGPD à charge des sous-traitants, notamment pour ce qui est des obligations documentaires (dont le registre des opérations de traitement), des annonces en cas de failles de sécurité, des obligations de sécurité ou encore des actes qui seraient rendus nécessaires par l'exercice des droits de la personne concernée[79]. Partant du contenu requis par l'art. 28 par. 3 RGPD, le contrat ainsi conclu devra explicitement imposer au sous-traitant l'essentiel des obligations qui lui reviendraient s'il était directement soumis au RGPD. Comme les LD 3/2018 le confirment expressément, une soumission « indirecte » au RGPD en découlera donc pour le sous-traitant[80].

[47] La distinction entre une soumission « directe » et « indirecte » est d'importance, dans la mesure où seules les obligations qui seraient contractuellement imposées au sous-traitant s'appliqueront, à l'exclusion des autres obligations que le RGPD lui met à charge en cas d'application directe. Ainsi, le sous-traitant n'aura pas à nommer un représentant dans l'EEE (art. 27 RGPD), à tenir un registre des activités de traitement (art. 30 par. 2 RGPD – en tout cas si ceci n'est pas exigé contractuellement de la part du responsable du traitement), à nommer un délégué à la protection des données à caractère personnel (art. 37 et 38 RGPD) ou encore à coopérer avec l'autorité (art. 31 RGPD). De même, il ne sera pas formellement soumis au risque d'amendes administratives de l'art. 83 RGPD, en raison justement du fait que le RGPD ne lui est pas directement applicable. Dans l'ensemble, seule la responsabilité contractuelle à l'égard du responsable du traitement – de même que, théoriquement, la responsabilité civile à l'égard de la personne concernée ou de toute autre personne qui serait lésée par ses agissements ou omissions – se posera en cas de problème. Il faut finalement encore relever que ces obligations ne concernent pas tous les traitements de données, mais seulement ceux effectués dans le cadre du contrat de sous-traitance.

(ii) Le responsable du traitement soumis au RGPD par l'application extraterritoriale de l'art. 3 par. 2 RGPD

[48] Dans cette seconde hypothèse, ni le sous-traitant ni le responsable du traitement ne disposent d'un établissement dans l'EEE, de sorte qu'aucun d'eux n'est soumis au RGPD « territorialement » par l'art. 3 par. 1 RGPD. En revanche, il est possible que le responsable du traitement soit pour sa part soumis extraterritorialement au RGPD par son art. 3 par. 2. Comme dans le cas précédent, le responsable du traitement se verrait directement appliquer le RGPD pour les traitements en

78 LD 3/2018, p. 11.

79 LD 3/2018, p. 11.

80 Ce caractère indirect est explicitement relevé aux LD 3/2018, p. 11.

question, alors que le sous-traitant devrait se voir imposer contractuellement les obligations qui permettent au responsable du traitement de respecter ses propres devoirs.

[49] Pourtant, et sans explication réelle, les LD 3/2018 retiennent dans cette seconde hypothèse une autre solution que pour la première. À teneur de ce texte en effet, le sous-traitant devrait lui-même directement et personnellement être soumis au RGPD si le responsable du traitement l'est par le truchement de l'art. 3 par. 2 RGPD[81]. Plus précisément, il y est considéré que cette application directe du RGPD au sous-traitant intervient par application de l'art. 3 par. 2 RGPD, dès le moment où le traitement de données à caractère personnel confié au sous-traitant par le responsable du traitement fait lui-même tomber celui-ci dans le champ d'application territoriale du RGPD. Ainsi, si le sous-traitant doit exécuter un traitement de données à caractère personnel pour le compte du responsable du traitement qui réaliserait les critères de l'art. 3 par. 2 RGPD, tant le responsable du traitement que le sous-traitant lui-même se verraient soumettre à titre personnel au RGPD.

[50] Dans les LD 3/2018, il est bien noté que seul le responsable du traitement décide du but et des moyens du traitement, lesquels constituent les éléments centraux du critère du « ciblage » retenu à l'art. 3 par. 2 RGPD. Cependant, il y est explicitement noté que cela n'exclut pas le fait que le sous-traitant puisse activement prendre part dans l'activité de traitement en question – et donc dans le ciblage. Et que, de ce fait, il réalise à titre personnel les conditions de l'art. 3 par. 2 RGPD.

[51] Ce raisonnement étonne naturellement à plus d'un titre et ne peut être que difficilement suivi.

[52] D'abord, et principalement, par le fait qu'il amène à un résultat complètement différent de celui qui est retenu dans les mêmes LD 3/2018 dans le cas où le responsable du traitement est soumis au RGPD par son art. 3 par. 1. On l'a vu, il est dans ce cas explicitement retenu que le sous-traitant doit *contractuellement* être soumis à certaines obligations minimales exigées par le RGPD, dans la mesure où ce dernier ne lui est pas directement applicable. Or, aucune explication n'est donnée quant aux motifs expliquant cette différence de traitement. Ceci alors que, dans les faits, un rattachement du responsable du traitement par l'art. 3 par. 1 RGPD sera plus étendu que celui issu de l'art. 3 par. 2 RGPD – de sorte que les risques pour les personnes concernées dans l'EEE peuvent également être plus marqués, par le nombre de personnes impliquées ou la diversité des traitements mis en œuvre.

[53] Ensuite, cette solution méconnaît le fait que le sous-traitant n'est justement pas celui qui *vise* le marché européen au sens là également pourtant décrit et détaillé dans les LD 3/2018, c'est-à-dire (en tout cas pour l'offre de biens et de services) en choisissant de cibler les personnes dans l'EEE. Cette décision et l'identification tant du but que des modalités du traitement sont le fait unique du responsable du traitement – un élément qui est d'ailleurs expressément relevé dans les LD 3/2018[82]. Dès lors que ce n'est pas lui qui décide de ce ciblage, l'on ne saurait faire application de l'art. 3 par. 2 RGPD à son égard, ceci même s'il prend part – en son rôle de sous-traitant – au traitement de données pertinent selon cette disposition. En effet, ce ne serait que dans le cas où il serait lui-même responsable du traitement qu'une application directe du RGPD à son égard serait envisageable.

81 LD 3/2018, pp. 20–22.

82 LD 3/2018, p. 21.

[54] Enfin, cette application directe du RGPD à l'égard du sous-traitant entraîne pour lui des risques particulièrement marqués sans même qu'il puisse être en mesure d'en connaître l'existence. Par son rôle restreint et les limites qui doivent entourer ses propres traitements de données à caractère personnel, le sous-traitant ne sera le plus souvent pas à même de savoir que le critère de l'art. 3 par. 2 RGPD est réalisé par le responsable du traitement, soit car il n'a pas lui-même accès au détail des données à caractère personnel traitées (par exemple dans le cas d'un service d'hébergement), soit car il ne peut sur cette seule base juger de la réalisation du critère du *ciblage*. Or, sans savoir cela, le sous-traitant n'est naturellement pas en mesure de savoir si le RGPD lui est ou non directement applicable[83].

[55] Si l'on prend l'exemple d'un sous-traitant offrant des services d'hébergement (*cloud*) pour des données récoltées et traitées par le responsable du traitement d'une façon entrant dans le cadre de l'art. 3 par. 2 RGPD, ce service servirait directement au traitement précité. En conséquence, il mènerait à l'application directe du RGPD au sous-traitant également, en suivant le principe posé dans les LD 3/2018. Or, en tant qu'il ne fait qu'héberger les données sans les analyser, le sous-traitant ne saura pas que celles-ci entrent dans le cadre de l'art. 3 par. 2 RGPD. Pire, il est probable – car justement requis par l'art. 28 RGPD – que le sous-traitant doive *contractuellement* éviter tout traitement des données à caractère personnel autre que le seul hébergement, dont toute analyse des données lui permettant de savoir qu'elles concernent des personnes dans l'EEE. La limitation du traitement ainsi imposée, qui permet au responsable du traitement de garantir la sécurité des données et la proportionnalité du traitement, empêcherait justement toute possibilité pour le sous-traitant d'identifier les obligations qui lui reviennent.

[56] Si du point de vue des autorités de contrôle, on peut comprendre l'envie de soumettre un maximum d'acteurs au RGPD, y compris les sous-traitants et responsables de traitement hors EEE, le raisonnement tenu dans les LD 3/2018 spécifiquement pour le cas où le responsable du traitement est soumis au RGPD par son art. 3 par. 2 n'est juridiquement pas acceptable, parce qu'il ne correspond pas à la solution trouvée dans le cas du rattachement par l'art. 3 par. 1 RGPD et parce que l'entier du paragraphe a été ajouté sans explications après la consultation publique[84]. À notre connaissance, cette disposition n'a pas encore fait l'objet de jurisprudence et est passée relativement inaperçue dans la doctrine. On peut donc légitimement se demander quelle portée il faut réellement accorder à cet emballement (ou faudrait-il dire cet égarement de l'EDPB), bien que cela reste un risque pour les sous-traitants, à évaluer de manière prudente.

[57] S'il est vrai que l'art. 3 par. 2 RGPD mentionne explicitement le sous-traitant, cette référence porte justement sur le *traitement* qui est soumis au RGPD – et non sur la personne l'opérant. Ce point est rappelé dans plusieurs des passages des LD 3/2018[85]. Ainsi, en faisant référence aux traitements « *par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union* », l'art. 3 par. 2 RGPD vise vraisemblablement exclusivement à s'assurer que le responsable du traitement hors de l'EEE soumis au RGPD ne puisse pas sortir du champ d'application de cette règle uniquement au motif qu'il ne ferait pas lui-même le traitement, mais que celui-ci aurait été confié à un sous-traitant. En d'autres termes, c'est bien le traitement qui relève du RGPD –

83 La seule solution pour le sous-traitant serait d'exiger du responsable du traitement une garantie contractuelle qu'il n'est pas soumis au RGPD. Si le responsable du traitement devait quand même y être soumis, le sous-traitant pourrait faire valoir une violation du contrat à l'égard du responsable du traitement. Cela ne réduirait pourtant guère sa propre responsabilité aux yeux d'une autorité de contrôle.

84 Au contraire du passage concernant l'art. 3 par. 1 RGPD.

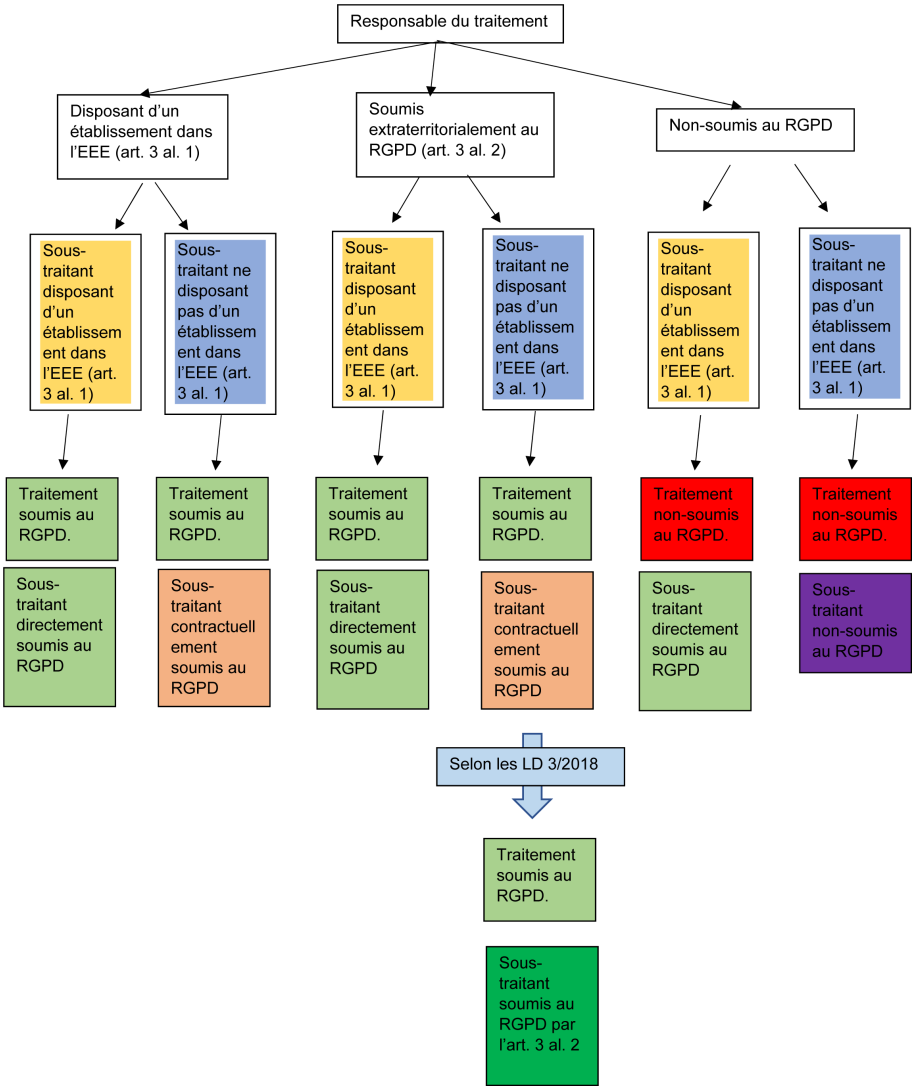
85 LD 3/2018, pp. 5 et 14.

et qui déclenche les obligations du responsable du traitement – et non la personne qui l'opère. Cette interprétation de la référence au « sous-traitant » à l'art. 3 par. 2 RGPD apparaît d'ailleurs en ligne avec le fait historique que cette référence a été ajoutée en cours de débats, sur proposition du Parlement européen. Ce faisant, le Parlement européen n'a pas nécessairement identifié les conséquences réelles de cet ajout ni le cadre complet dans lequel il s'inscrivait, souhaitant uniquement faire correspondre ces références à celles données au par. 1 précédent.

[58] Partant, nous sommes d'avis que la solution à appliquer dans ce cas doit être identique à celle retenue dans le cas où le responsable du traitement est soumis au RGPD par l'art. 3 par. 1, soit le fait que le sous-traitant n'est lui-même pas *directement* soumis au RGPD, mais doit être *contractuellement* contraint d'en respecter les obligations. Sur ce point donc, les LD 3/2018 ne sauraient être suivies.

3.3.3. Schéma résumant les cas d'application du RGPD au sous-traitant

[59] A la lumière des points qui précèdent, nous proposons – à titre illustratif – le schéma suivant permettant de mieux comprendre les différentes hypothèses se posant :



4. Conclusion

[60] Le RGPD a prévu des hypothèses d'application territoriales et extraterritoriales larges pour s'assurer que ses règles puissent être imposées au plus grand nombre de responsables du traitement et de sous-traitants. Cela commence par une soumission de tous les responsables du traitement établis sur le territoire de l'EEE (ou un territoire où le droit s'applique par renvoi du droit international public), indépendamment du lieu réel du traitement ou des personnes concernées (art. 3 par. 1 et 3 RGPD). S'ensuit une application extraterritoriale au responsable du traitement qui vise le marché de l'EEE ou y effectue du profilage en ligne, pour les seules données liées à ces activités (art. 3 par. 2 RGPD), ainsi que la soumission à certaines dispositions du RGPD au sous-traitant par voie contractuelle (pour les traitements soumis au RGPD à raison du responsable du traitement).

[61] Malgré ces hypothèses déjà bien extensives, l'EDPB a ajouté à la dernière minute dans les LD 3/2018 une soumission directe du sous-traitant au RGPD lorsque son responsable du traitement est soumis de manière extraterritoriale. À notre avis, cela ne correspond ni à la lettre, ni à l'esprit du RGPD, mais plutôt à une volonté des autorités de contrôle d'étendre leur emprise, sans fondement ni justification légale. Et d'une façon qui entraîne un risque direct pour le sous-traitant, sans qu'il ne puisse pour autant en juger de l'étendue.

Sylvain Métille est Professeur associé, Directeur de la Maîtrise universitaire en Droit, criminalité et sécurité des technologies de l'information (M DCS) et Membre de la Commission d'éthique de la recherche de l'Université de Lausanne. Il enseigne et est le responsable scientifique du Certificate of Advanced Studies en Protection des données d'UniDistance. Docteur en droit, il est également avocat associé à l'Étude HDC à Lausanne.

David Raedler est avocat au sein de l'Étude HDC à Lausanne et vice-président du Tribunal de prud'hommes de La Broye et du Nord vaudois. Docteur en droit sur le sujet des enquêtes internes, il enseigne également notamment dans le Certificate of Advanced Studies en Protection des données d'UniDistance au sujet des obligations du responsable du traitement.

Les auteurs remercient M. Livio di Tria, assistant diplômé à l'Université de Lausanne, pour sa relecture attentive et son aide pour l'appareil critique.